A Novel ICMetric Based Framework for Securing the Internet of Things

Ruhma Tahir, Hasan Tahir, Klaus McDonald-Maier, *Anil Fernando
School of Computer Science and Electronic Engineering, University of Essex, Colchester
rtahir@essex.ac.uk, htahir@essex.ac.uk, kdm@essex.ac.uk
*Centre for Vision, Speech and Signal Processing, University of Surrey, Guildford
w.fernando@surrey.ac.uk

***Abstract* — Over the years IoT has gained importance and is rapidly evolving. Security and privacy issues have been described as the most challenging problems in the IoT domain. Security at both the device and network level is critical to the operation of IoT. Our proposed novel ICMKeyStream framework aims to safeguard against threats at the device and network level; thereby providing authentication, confidentiality and non-repudiation for continuous data streams as with many IoT applications. The evaluation of our system proves that our scheme is very feasible for the embedded system devices driving the IoT.**

I. Introduction

Popularity of internet enabled devices has resulted in the creation of a new technological advancement called internet of things (IoT). IoT allows heterogeneous internet devices to collaborate with each other thus enabling data and information sharing. An advantage of this environment is that it encourages interactions between the digital and physical world to fulfill the demand for increased connectivity. When data moves across multiple networks and devices, the chance of a security failure rises considerably [1]. Commercial pressures have forced the development of IoT enabled devices that do not possess the ability or the resources to provide security.

Traffic in the IoT may be protected while it is in transit but there is still need to protect the embedded system found in IoT devices [2]. ICMetric [3] is a recent innovation in the field of cryptography that resolves issues related to key compromise in modern systems. In this paper, a novel scheme has been presented based on the ICMetric technology coupled with Secure Remote Rabbit Protocol, which secures entities and their intercommunications to provide security for the IoT. The proposed novel ICMKeyStream framework safeguards against device and network level threats. At the device level, our scheme uses ICMetric key generation that safeguards from device cloning, device tampering and unauthorized access. At the network level, our scheme provides authentication and secure transmission of continuous data streams between entities in IoT applications, while safeguarding from pre-computed attacks. Tests show that our framework provides these functionalities at the cost of minimal time and memory consumption.

II. Integrated Circuit Metric (ICMetric)

A cryptographic scheme is considered secure if the keys are kept secret. ICMetric is a technology that attempts to resolve issues related to key theft by generating an ICMetric (identification) using the inherent features of a device. An ICMetric is associated with the cryptographic keys of a device which implies that there is no need to store the keys on the system. The ICMetric of a device is generated only when a key is required. After use the ICMetric is discarded thus eliminating any chances of key theft/ capture. What sets the ICMetric technology apart is the fact that no ICMetric data/ template is stored on the system.

Generation of the ICMetric for a device is a mathematical and statistical process. When generating the ICMetric for a device we use a set of features which are difficult to capture or replicate by an attacker. Besides this the features should be stable and repeatable. The choice of features plays a crucial role in the security of the device ICMetric. For instance the MAC address or the IP address of a device are not a suitable option since both can be extracted using network monitoring tools and then spoofed to imitate a target device.

The ICMetric generation is a two-step process i.e. calibration phase and operation phase. In the calibration phase features of a device are extracted and processed mathematically and statistically. The results of this phase are processed in the operation phase. In this phase, a final ICMetric is generated for a device. The final ICMetric is generated by either adding the individual feature values or by concatenating the individual feature values.

An advantage of using the ICMetric technology is that it can be used for preventing device cloning, device tampering and unauthorized access. The ICMetric technology adds an extra layer to existing cryptographic schemes in an attempt to eliminate problems related to key theft and device cloning.

III. ICMKeystream Design

The following section details the steps involved in the secure functioning of our novel ICMKeyStream framework and fig 1 shows its overall working.

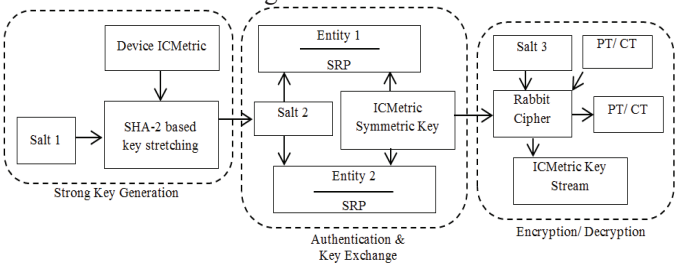


Figure 1. Working of ICMKeyStream

A. Strong ICMetric Key Generation

The ICMetric is of insufficient length and entropy, to serve as a key for cryptographic operations. This module of the scheme performs multiple iterations of the key derivation

function, on ICMetric coupled with a salt to generate a strong symmetric ICMetric key.

Strong Key = SHA-2(ICMetric no, 128 bit salt value)

B. Authentication and Key Exchange

The design of our ICMetric key exchange and authentication scheme is based on the Secure Remote Password Protocol. SRP is particularly suitable for our application and doesn't require the exchange of ICMetric information between parties. Entity A and B create symmetric key based on A's ICMetric value and cryptographic verifier derived from IC_A.

$$A = g^a \bmod N, B = k \cdot v + g^b$$

Then both entities generate identical random scrambler's $u = h(A \mid B)$ based on the shared ephermal values A and B. Entity A generates the symmetric key,

$S_A = (B - kv)^{a+ux}$, $K_A = h(S_A)$

Entity B generates the same symmetric key.

$S_B = (A \cdot v^u)^b$, $K_B = h(S_B)$

C. ICMetric Encryption/ Decryption

Rabbit stream cipher [4] is used to provide encryption/decryption to continuously streamed data signals, thereby achieving data confidentiality between entities forming the IoT network. The key and IV setup schemes are based on the ICMetric symmetric key to generate an ICMetric keystream for performing secure communications.

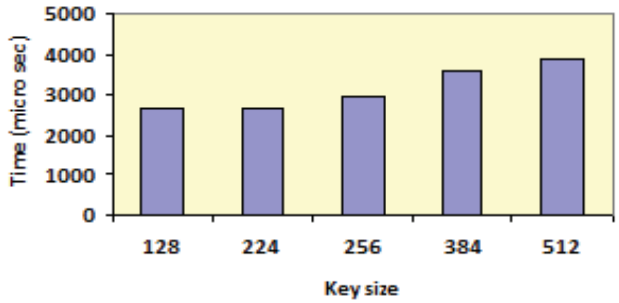
IV. Results and Analysis

A. Experimental Results

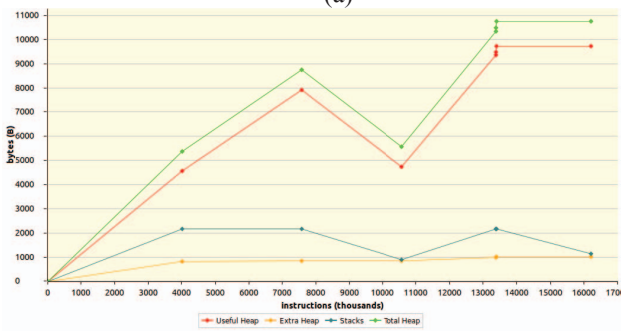
Our framework is implemented using C on Linux, Intel Corei3 3.2 GHz processor with 6GB RAM. The authentication, key generation and encryption/decryption modules are implemented using OpenSSL cryptographic library, and evaluated based on RAM and running time. Figure 2(a) shows time taken by the authentication and key exchange module, showing five variants 128, 224, 256, 384, 512 bit. The graph in figure 2(b), depicts memory profile of 128 bit variant by presenting program lifecycle and the memory consumed. The encryption/ decryption module takes 14 microseconds and maximum total memory consumed for the encryption/ decryption using 128-bit ICMetric key is around 3.9KB for iteration as evident from figure 2(c). It is evident from graphs that our scheme is able to provide higher levels of security without substantial time and memory performance overheads.

B. Security Analysis

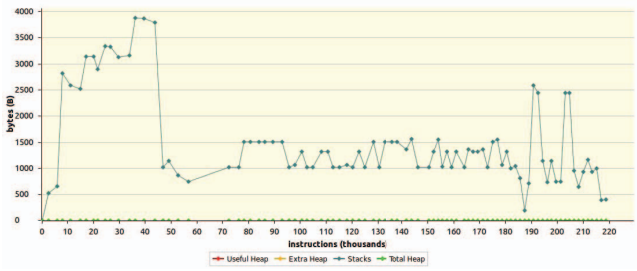
The data sent by each entity is encrypted using Rabbit cipher based on the ICMetric symmetric keystreams. This property is particularly important since most of the applications in the IoT rely on continuous encrypted streams of data, enabling authenticated parties that are in possession of a symmetric key to access data. Our framework deters all forms of key capturing, since both the ICMetric and the cryptographic keys are discarded after operation. The symmetric key generation module uses key derivation functions on ICMetric coupled with a salt, to provide strong symmetric ICMetric key, thereby safeguarding from various pre-computed attacks. Our framework is a zero knowledge password proof which implies that at no point is the ICMetric be transmitted over the channel for the purpose of authentication and key exchange.



(a)



(b)



(c)

Figure 2. (a) Running time for ICMetric symmetric key variants. (b) RAM consumption 128-bit ICMetric symmetric key(c) RAM consumption ICMetric encryption/decryption

V. Conclusion

Our novel ICMKeyStream framework has been designed and optimized for the new and extremely complex embedded applications driving the Internet of Things. Our framework combines the security advantages of the device ICMetric and the designed symmetric key generation scheme for the providing confidentiality, authentication and non-repudiation between the entities. We have been able to prevent major threats like key theft, man-in-the-middle attack and brute force attack related to secure communication of data.

References

[1] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *IEEE Computer*, vol. 44, no. 9, pp. 51-58, 2011.

[2] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the Internet of Things: A Standardization Perspective," *IEEE Internet of Things Journal*, vol. 1, no. 3, pp. 265-275, 2014.

[3] E. Papoutsis, "Investigation of The Potential of Generating Encryption Keys For ICMetrics," The University of Kent, PhD Thesis 2009.

[4] M. Boesgaard, M. Vesterager, T. Pedersen, J. Christiansen, and O. Scavenius, "Rabbit: A High-Performance Stream Cipher," in *LNCS 2887*.: Springer, 2003, pp. 307-329.